



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,068	12/03/2003	Robert E. Cavanaugh	58895/P003US/10305848	5018
29053 7590 09/02/2008 FULBRIGHT & JAWORSKI L.L.P. 2200 ROSS AVENUE SUITE 2800 DALLAS, TX 75201-2784				
EXAMINER TRUONG, THANHNGA B				
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
09/02/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/727,068

Applicant(s)

CAVANAUGH, ROBERT E.

Examiner

Thanhnga B. Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 June 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/ICE)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is responsive to the communication filed on June 06, 2008. Claims 1-43 are pending. At this time, claims 1-43 are still rejected.

Response to Arguments

2. Applicant's arguments filed June 06, 2008 under **35 USC § 101** have been fully considered but they are not persuasive at least for claims 13-19.

Applicant argues that claim 13 is statutory and cannot give a specific reason of where in the specification that supports this computer program product, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Besides, applicant insists that he/she does not require to define or point out a specific area of the specification that could clearly support "computer readable medium", which again is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Examiner respectfully disagrees with the applicant and still maintain the rejection of claims 13-19 under **35 USC § 101**.

With regard to claim 13, the computer program product having a computer readable medium having computer program is not clearly define any where in the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Moreover, the claimed language direct clearly toward a computer program, which is not patentable. Besides, the specification does mention various computer programs and systems have been developed to facilitate such information communication (see paragraph 0003 of the specification). Thus claim 13 is a non-statutory.

Claims 14-19 are depended on claim 13, thus they are rejected with the same rationale applied against claim 13 above.

For the above reasons, it is believed that the rejections for claims 13-19 under **35 USC § 101** should be sustained.

Applicant's arguments filed June 06, 2008, with respect to the rejection(s) of claim(s) 1-43 under **35 USC § 103** have been fully considered but they are not persuasive.

Applicant has argued that:

The combination of teaching between Muttik and Kouznetsov fails to teach "a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient., said malicious code analyzer being configured to be transparent to systems of said communication system", as recited in claim 1 of the invention.

Examiner respectfully disagrees with the applicant and still maintains that:

Muttik does teach malicious behavior by analyzing patterns of systems calls made during emulation of the software. The system operates by emulating the software within an insulated environment in a computer system so that the computer system is insulated from malicious actions of the software. During the emulation process, the system records a pattern of system calls directed to an operating system of the computer system. The system compares the pattern of system calls against a database containing suspect patterns of system calls. Based upon this comparison, the system determines whether the software is likely to exhibit malicious behavior. In one embodiment of the present invention, if the software is determined to be likely to exhibit malicious behavior, the system reports this fact to a user of the computer system. In one embodiment of the present invention, the process of comparing the pattern of system calls is performed on-the-fly as the emulation generates system calls (see abstract as well as Figure 2 of Muttik). Although Muttik teaches a system for providing protection against malicious code (see Figure 2 of Muttik), Muttik is silent on the capability of showing the malicious code analyzer being configured

to be transparent to systems of said communication system. On the other hand, Kouznetsov teaches this limitation in column 13, lines 22-29 of Kouznetsov).

Besides, applicant recited the language, "between **an originator** of an information communication of said communication system traffic pattern and an intended recipient", wherein **an originator** does not clearly support anywhere by the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Examiner, however, noticed that paragraph [0009] of the specification does talk about recipient received electronic email which could contain code, which also met in Figures 2 and 3 of Muttik.

In addition, applicant recited the language, "malicious code analyzer being configured to be transparent to systems of said communication system", wherein **transparent to systems** does not clearly support by the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. However, Examiner does see that malicious code which is transparent to network users is shown in paragraph [0020], which also teaches in column 13, lines 22-29 of Kouznetsov. Thus the combination of teaching between Muttik and Kouznetsov teaches the claimed subject matter.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, according to the response that has been addressed above, the combination of teaching between Muttik and Kouznetsov is efficient and proper.

Applicant further argued that:

Art Unit: 2135

Muttik does not teach "wherein said malicious code analyzer comprises: code for identifying unwanted or unsolicited messages", as recited in claim 9.

Examiner respectfully disagrees with the applicant and still maintains that:

Muttik teaches in column 3, lines 49-53 that before executing code 108, computer system 106 uses emulator 110 to analyze code 108. This analysis involves examining a pattern of system calls (API calls) generated by code 108 in order to detect potentially malicious behavior, wherein malicious behavior is the unwanted or unsolicited messages. Any abnormal behavior, such as, unwanted or unsolicited messages, is considered malicious behavior.

Applicant further argued that:

Muttik does not teach "communications throttle for determining if said information communication is to be passed by said system", as recited in claim 11.

Examiner respectfully disagrees with the applicant and still maintains that:

Muttik does teach in column 4, lines 8-11 that Comparison unit 204 produces a decision 212, which indicates whether or not the code is likely to exhibit malicious behavior, which is clearly shown the "IF" condition whether or not to pass the information communication as recited in claim 11.

Claims 13, 20 and 30 contain limitations that are similar to that of claims 1 and 10, thus they are rejected with the same rationale applied against claims 1 and 10 above.

Muttik, Kouznetsov, Mathon, and Desai do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior

art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative, should not be construed as indicating Examiner's agreement therewith.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 13-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- a. *Referring to claim 13:*

Claim 13 recites "a computer program product for providing protection against malicious code." It appears that there is no process, machine, manufacture, or composition of matter in the claimed language. These claims are clearly directed toward a software program and they are non-statutory as not being tangibly embodied in a manner so as to be executable. Furthermore, the computer program product having a computer readable medium having computer program is not well define any where in the specification, and the claimed language direct clearly toward a computer program. Besides, the specification does mention various computer programs and systems have been developed to facilitate such information communication (see paragraph 0003 of the specification). Thus, claim 13 is a non-statutory. Please see "Response to Argument" that has been addressed above.

Claims 14-19 are depended on claim 13, thus they are rejected with the same rationale applied against claim 13 above.

Claim Rejections - 35 USC § 103

Art Unit: 2135

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3, 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik (US 6,775,780 B1), and further in view of Kouznetsov et al (US 7,096,501 B2).

a. Referring to claim 1:

i. Muttik teaches a system for providing protection against malicious code (see Figure 2 of Muttik):

(1) a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication to intercept said information communication and to analyze said information communication for malicious code, said malicious code analyzer being configured to be transparent to systems of said communication system (**see Figure 2, element 108 and column 1, line 65 through column 2, line 11 of Muttik**).

ii. Although Muttik teaches a system for providing protection against malicious code (see Figure 2 of Muttik), Muttik is silent on the capability of showing the malicious code analyzer being configured to be transparent to system of said communication system. On the other hand, Kouznetsov teaches this limitation in column 13, lines 22-29 of Kouznetsov).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Muttik with the teaching of Kouznetsov or detecting malicious software by analyzing patterns of system calls generated by the software during emulation (**column 1, lines 10-12 of Muttik**).

iv. The ordinary skilled person would have been motivated to: (1) have modified the invention of Muttik with the teaching of Kouznetsov to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software **(column 1, lines 59-63 of Muttik).**

b. Referring to claim 3:

i. Muttik further teaches:

(1) wherein said transparent configuration of said malicious code analyzer comprises: a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer **(column 1, lines 40-47; column 3, line 65 through column 4, line 11 of Muttik).**

c. Referring to claim 8:

i. The combination of teaching between Muttik and Kouznetsov teaches the claimed subject matter. Kouznetsov further teaches:

(1) wherein said malicious code analyzer comprises: code for virus scanning **(column 1, lines 42-44, column 4, lines 37-38 of Kouznetsov).**

d. Referring to claim 9:

i. Muttik further teaches:

(1) wherein said malicious code analyzer comprises: code for identifying unwanted or unsolicited messages **(column 3, lines 49-52 of Muttik).**

e. Referring to claim 11:

i. Muttik further teaches:

(1) a communications throttle for determining if said information communication is to be passed by said system **(see Figure 2, element 212 and column 4, lines 8-11 of Muttik).**

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik (US 6,775,780 B1), in view of Kouznetsov et al (US 7,096,501 B2), and further in view of Desai et al (US 7,203,192 B2).

a. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

ii. Although the combination of teaching between Muttik and Kouznetsov teaches the claimed subject matter, they are not clear and/or silent on the capability of showing the steering module. On the other hand, Desai teaches this limitation in column 3, lines 14-27 of Desai.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Muttik with the teaching of Desai or detecting malicious software by analyzing patterns of system calls generated by the software during emulation (**column 1, lines 10-12 of Muttik**).

iv. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Muttik with the teaching of Desai to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software (**column 1, lines 59-63 of Muttik**).

8. Claims 13-14, 16-22, 26-34, 40-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik (US 6,775,780 B1), and further in view of Desai et al (US 7,203,192 B2).

a. Referring to claim 13:

i. This claim consist a computer program product having a computer readable medium having computer program logic recorded thereon for providing protection against malicious code to implement claims 1

Art Unit: 2135

(without the transparency) and 10; thus it is rejected with the same rationale applied against claims 1 (without the transparency) and 10 above.

b. Referring to claim 14:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

c. Referring to claims 16, 26:

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

d. Referring to claims 17, 27:

i. These claims have limitations that is similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

e. Referring to claims 18, 28:

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

f. Referring to claims 19, 29:

i. These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

g. Referring to claim 20:

i. Muttik teaches a method for providing protection against malicious code (see Figure 2 of Muttik):

(1) intercepting packets in an information communication traffic pattern (**column 4, lines 59-64; column 5, lines 1-13 of Muttik**);

(2) analyzing said at least a portion of said packets by said malicious code analyzer before releasing said at least a portion of said packets back into said traffic pattern **(column 3, lines 54-57 of Muttik)**.

ii. Although Muttik teaches the method for providing protection against malicious code, Muttik is not clear and/or silent on the capability of steering said packets between interfaces associated with an information communication originator and said intended recipient, said steering providing detouring of at least a portion of said packets to a malicious code analyzer. On the other hand, Desai teaches this limitation in the abstract and in column 3, lines 8-30 of Desai.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Muttik with the teaching of Desai or detecting malicious software by analyzing patterns of system calls generated by the software during emulation **(column 1, lines 10-12 of Muttik)**.

iv. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Muttik with the teaching of Desai to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software **(column 1, lines 59-63 of Muttik)**.

h. Referring to claim 21:

i. This claim has limitations that is similar to those of claim 20, thus it is rejected with the same rationale applied against claim 20 above.

i. Referring to claim 22:

i. Muttik further teaches:

(1) wherein said protective system is disposed as a protected network edge device **(see Figure 1 and column 3, lines 22-53 of Muttik).**

j. Referring to claim 30:

i. This claim has limitations that is similar to those of claims 1 (without the transparency), 3, and 10, thus it is rejected with the same rationale applied against claims 1 (without the transparency), 3, and 10 above.

k. Referring to claims 31-34, 40-43:

i. These claims have limitations that is similar to those of claims 20-22 and 26-29, thus they are rejected with the same rationale applied against claims 20-22 and 26-29 above.

9. Claims 2, 4-7, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik (US 6,775,780 B1), in view of Kouznetsov et al (US 7,096,501 B2), and further in view of Mathon et al (US 7,032,005 B2).

b. Referring to claim 2:

i. Although the combination of teaching between Muttik and Kouznetsov teaches a system for providing protection against malicious code (see Figure 2 of Muttik), they are silent on the capability of not having a network address (e.g., zero footprint) associated therewith which is visible external to said system. On the other hand, Mathon teaches:

(1) wherein said transparent configuration of said malicious code analyzer comprises said malicious code analyzer not having a network address associated therewith which is visible external to said system **(column 7, lines 1-10 of Mathon).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Muttik with the teaching of Mathon to secure communication over the Internet **(column 1, lines 19-20 of Mathon).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Muttik with the teaching of Mathon to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software (**column 1, lines 59-63 of Muttik**).

b. Referring to claim 4:

i. Muttik and Mathon further teaches:

(1) wherein said malicious code analyzer comprises: a proxy (column 7, line 3 of Mathon) for emulating a behavior of a destination of said information communication (**column 3, lines 54-65 and column 4, lines 17-24 of Muttik**).

c. Referring to claim 5:

i. The combination of teaching between Muttik, Kouznetsov, and Mathon teaches the claimed subject matter. Mathon further teaches:

(1) wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system (**column 7, lines 1-10 of Mathon**).

d. Referring to claim 6:

i. The combination of teaching between Muttik, Kouznetsov, and Mathon teaches the claimed subject matter. Mathon further teaches:

(1) wherein said proxy comprises: server functionality; and client functionality (**column 7, line 3; column 3, line 7; column 9, lines 20-35 of Mathon**).

e. Referring to claim 7:

Art Unit: 2135

i. The combination of teaching between Muttik, Kouznetsov, and Mathon teaches the claimed subject matter. Mathon further teaches:

(1) a loop back interface for interfacing said information communication with said malicious code analyzer (**column 1, lines 40-47 of Muttik; column 3, line 35 of Mathon**).

f. Referring to claim 12:

i. The combination of teaching between Muttik, Kouznetsov, and Mathon teaches the claimed subject matter. Mathon further teaches:

(1) wherein said information communication conforms to a protocol selected from the group consisting of: simple mail transfer protocol (SMTP); post office protocol (POP); hypertext transfer protocol (HTTP); Internet message access protocol (IMAP); file transfer protocol (FTP); domain name service (DNS); hot standby router protocol (HSRP); open shortest path first (OSPF); and enhanced interior gateway routing protocol (EIGRP) (**column 7, line 32 of Mathon**).

10. Claims 15, 23-25, and 35-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik (US 6,775,780 B1), in view of Desai et al (US 7,203,192 B2), and further in view of Mathon et al (US 7,032,005 B2).

g. Referring to claim 15:

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

h. Referring to claim 23:

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

i. Referring to claim 24:

Art Unit: 2135

i. This claim has limitations that is similar to those of claims 3 and 4, thus it is rejected with the same rationale applied against claims 3 and 4 above.

j. Referring to claim 25:

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

k. Referring to claims 35-39:

i. These claims have limitations that is similar to those of claims 7 and 23-25, thus they are rejected with the same rationale applied against claims 7 and 23-25 above.

Conclusion

11. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-

Art Unit: 2135

3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/

Primary Examiner, Art Unit 2135

TBT

August 29, 2008